CLAIMS

What is claimed is:

1. A method for migrating a base chip key from a first computer system to a second computer system, wherein said first computer system includes a base chip key 1, and said second computer system includes a base chip key 2, said method comprising:

generating a second certificate for said base chip key 1 by a manufacturer of said second computer system using a first certificate for said base chip key 1, and generating a second certificate for said base chip key 2 by a manufacturer of said first computer system using a first certificate for said base chip key 2;

sending a first data packet from said first computer system to said second computer system, wherein said first data packet includes all data necessary to reproduce said base chip key 1 in said second computer system;

sending a second data packet from said second computer system to said first computer system acknowledging the receipt of a copy of said base chip key 1;

erasing said base chip key 1 from said first computer system; and

replacing said base chip key 2 in said second computer system with said base chip key 1.

2. The method of Claim 1, wherein said first data packet includes a first random number.

3. The method of Claim 1, wherein said first data packet is encrypted with said base chip key 1's public key.

4. The method of Claim 1, wherein said second data packet includes said first random number and a second random number.

5. The method of Claim 1, wherein said second data packet is signed by said base chip key 2.

6. The method of Claim 1, wherein said method further includes:

generating an identity key 1 in said first computer system, and generating an identity key 2 in said second computer system;

generating a certificate for said identity key 1, and generating a certificate for said identity key 2; and

generating a first certificate for said base chip key 1 using said identity key 1, and generating a first certificate for said base chip key 2 using said identity key 2.

7. A computer program product residing on a computer usable medium for migrating a base chip key from a first computer system to a second computer system, said computer program product comprising:

program code means for generating a second certificate for said base chip key 1 by a manufacturer of said second computer system using a first certificate for said base chip key 1, and generating a second certificate for said base chip key 2 by a manufacturer of said first computer system using a first certificate for said base chip key 2;

program code means for sending a first data packet from said first computer system to said second computer system, wherein said first data packet includes all data necessary to reproduce said base chip key 1 in said second computer system;

program code means for sending a second data packet from said second computer system to said first computer system acknowledging the receipt of a copy of said base chip key 1;

program code means for erasing said base chip key 1 from said first computer system; and

program code means for replacing said base chip key 2 in said second computer system with said base chip key 1.

8. The computer program product of Claim 1, wherein said first data packet includes a first random number.

9. The computer program product of Claim 1, wherein said first data packet is encrypted with said base chip key 1's public key.

10. The computer program product of Claim 1, wherein said second data packet includes said first random number and a second random number.

11. The computer program product of Claim 1, wherein said second data packet is signed by said base chip key 2.

12. The computer program product of Claim 1, wherein said computer program product further includes:

program code means for generating an identity key 1 in said first computer system, and generating an identity key 2 in said second computer system;

program code means for generating a certificate for said identity key 1, and generating a certificate for said identity key 2; and

program code means for generating a first certificate for said base chip key 1 using said identity key 1, and generating a first certificate for said base chip key 2 using said identity key 2.